BY ORDER OF THE COMMANDER
EDWARDS AIR FORCE BASE

AIR FORCE INSTRUCTION 31-401

EDWARDS AIR FORCE BASE
Supplement

6 DECEMBER 2013

Security

INFORMATION SECURITY PROGRAM MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-Publishing.af.mil** for downloading or ordering

RELEASABILITY: There are no releasability restrictions on this publication

OPR: 412 TW/IPII

Certified by: 412 TW/IP
(Stephen Gerteis)

Supersedes: AFI 31-401_ EDWARDSAFBSUP, 23 JAN 2008

Pages: 5

This publication supplements Air Force Instruction (AFI) 31-401, *Information Security Program Management*. It provides Edwards Air Force Base (EAFB) specific guidance and organizational responsibility for Information Security Program Management. This publication is applicable to all Air Force Units and Associate Tenant Units on Edwards Air Force Base (EAFB). This publication does not apply to Air Force Reserve Command (AFRC), Air National Guard (ANG), and Civil Air Patrol (CAP) Units. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) Refer recommended changes and questions about this publication to the Office or Primary Responsibility (OPR) using the AF IMT 847, *Recommendation for Change of Publication*; route AF IMT 847s from the field through the appropriate functional' s chain of command.

SUMMARY OF CHANGES

This document has been substantially revised and must be completely reviewed. Major changes include new organizational designations. This document aligns the revised Air Force Instruction 31-401, *Information Security Program Management, 1 November 2005*, and Air Force Materiel Command Supplement, *AFMC Information Security Program Management*, 16 April 2007.**AFI 31-401, 1 November 2005, is supplemented as follows.**

1.3.4. The Chief of Information Protection Office is the Information Security Program Manager (ISPM) for Edwards Air Force Base. The Chief delegates the duties of the ISPM and provides instruction, guidance and interpretation for implementing the DoD/AF Information Security Program for EAFB personnel.

1.3.5.1. Appoint security managers in writing. Include name, rank/grade, organization, office symbol, phone number, and level of security clearance in the appointment memorandum. Forward a copy of the appointment memorandum to 412 TW/IPII. Security managers must have a final clearance and access to the highest level of material managed by the organization.

1.3.6.2. Units with classified material must develop procedures specific to their organization that define: The processes to identify eligibility access, need-to-know; control of visitors when visits involve the disclosure of classified information; procedures on protection of classified material during an emergency; procedures to reduce the potential of accidental loss when small storage devices are authorized to store classified information; procedures for the daily security checks (end-of-day security checks); procedures for the internal control of classified material; procedures for when to change combinations to secure containers and rooms; procedures to ensure the control of reproduction of classified material; the removal and hand carrying of classified material, procedures for the incoming and outgoing shipment of classified material; procedures for the handling and safeguarding of CUI. If local procedures are developed, they must be included in the organization's security training.

1.3.8. 412 TW/IPAF is the Edwards OPR for the Foreign Disclosure Program.

1.3.9. Coordinate requests through AFTC/HO.

1.3.10. Security Container Custodian: A primary and alternate custodian will be appointed by branch or office chiefs to administer safes, vaults, or secure rooms.

1.4.2. Local Information Program Management Evaluations will be conducted by 412 TW/IP and coordinated with the security manager.

1.5.4. 412 TW/XP2 Special Security Office (SSO), manages the EAFB Sensitive Compartmented Information (SCI) Program.

1.5.5. 412 TW/IPS manages EAFB Special Access Programs.

1.6.1. 412 TW/IPI is the approval authority for requirements in this supplement.

1.6.4. Submit waivers through 412 TW/IPII.

1.7.1. 412 TW/IPII will consolidate data for the installation for submission by the due date.

1.7.1.1. 412 TW/IPII will alert unit security managers of data collection periods. Security managers will assemble data for their unit and submit it to 412 TW/IPII by the established suspense date.

1.8.1. Send reports through 412 TW/IPII.

3.6. Systematic Review for Declassification. Activities will review their classified holdings with a view towards declassification during their annual clean out day(s). This review pertains to classified holdings that were originally or derivatively classified by the activity.

5.5.2.2. Coordinate with 412 TW/IPAF before allowing access to classified information.

5.9.3. Include procedures for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, or terrorist activity, in local operating instructions or separate policy memorandum.

5.12.1. The Edwards Command Post (EAFB Command Post), Bldg. 2654, is the overnight repository for transient hand-carried classified material. Aircrews may use the EAFB Command Post or Base Operations.

5.14. Protecting classified on EAFB aircraft is an owner/user responsibility. Follow procedures to protect classified equipment and components installed on EAFB aircraft while on EAFB.

5.18.2. Submit justification for open storage to 412 TW/IPII prior to construction.

5.21.2. The first two names listed on the Standard Form 700, Security Container Information, are the primary and alternate "Security Container Custodian."

5.21.2.1. Post the form in the locking drawer so it is readily identifiable by anyone that may find the container or door open and unattended.

5.24.1. Unit commanders (or equivalents) and staff agency chiefs designate and approve reproduction equipment in writing.

5.28.1. Shredders and disintegrators used to destroy classified material must be verified on the National Security Agency (NSA) Approved Products List and approved, in writing, by the security manager prior to being used for the destruction of classified material. Post a copy of the security manager approval adjacent to the equipment. Label equipment as approved for destruction of classified material. Label all other destruction equipment as unapproved for classified use.

5.28.3. Edwards AFB does not have a Central Destruct Facility (CDF), organizations must budget and plan accordingly for the destruction of classified material.

6.1.7. **(Added-EAFB)** Accountable mail shall only be hand delivered to the intended recipient, do not leave accountable mail on an empty desk, unsecured drop box, or other unsecured location outside of the Activity Distribution Office (ADO). If undeliverable the ADO custodian shall secure all unopened undelivered accountable mail in a GSA-approved security container authorized for the storage of Secret material. Security managers must verify clearance level of ADO custodians by signing the AF Form 4332.

6.1.8. **(Added-EAFB)** All official incoming and outgoing accountable communications must be processed through the ADO in accordance with the DoD Mail Manual, this includes; Base Information Transfer System (BITS), U.S. Postal Service, and GSA commercial deliveries.

6.8. The local area is defined as the Installation of EAFB and does not include remote sites associated with the Installation.

8.9.2. Specialized refresher security training is included in security manger meetings and security awareness training material.

9.9.1.2. Inquiry officials must contact the 412 TW/IPII for a briefing before they start the inquiry. Bring a copy of the appointment memorandum to the briefing.

9.11.2. Contact 412 TW/IPII to receive an Edwards AFB incident number before appointing an investigative official.

MICHAEL T. BREWER,
Brigadier General, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

(Added) AFI 31-401, *Information Security Program Management*, 1 November 2005

(Added) DODM4225.8_AFMAN 33-306, *DOD Official Mail Manual*, 12 October 2006